ARIZONA STATEWIDE INFORMATION SECURITY	STATEWIDE POLICY	State of Arizona

STATEWIDE POLICY 8320: ACCESS CONTROLS

DOCUMENT NUMBER:	P8320
EFFECTIVE DATE:	JULY 1, 2015
REVISION:	DRAFT

1. AUTHORITY

To effectuate the mission and purposes of the Arizona Department of Administration (ADOA), the Agency shall establish a coordinated plan and program for information technology (IT) implemented and maintained through policies, standards and procedures (PSPs) as authorized by Arizona Revised Statutes (A.R.S.)§ 41-3504 and § 41-3507.

2. PURPOSE

The purpose of this policy is to define the correct use and management of logical access controls for the protection of state information systems and assets.

3. SCOPE

3.1 Application to Budget Units - This policy shall apply to all BUs as defined in A.R.S. § 41-3501(1).

3.2 Application to Systems -This policy shall apply to all state information systems:

- **a. (P)** Policy statements preceded by "(P)" are required for state information systems categorized as Protected.
- **b. (P-PCI)**Policy statements preceded by "(P-PCI)" are required for state information systems with payment card industry data (e.g., cardholder data).
- **c. (P-PHI)** Policy statements preceded by "(P-PHI)" are required for state information systems with protected healthcare information.
- **d. (P-FTI)** Policy statements preceded by "(P-FTI)" are required for state information systems with federal taxpayer information.

3.3 Information owned or under the control of the United States Government shall comply with the Federal classification authority and Federal protection requirements.

4. EXCEPTIONS

4.1 PSPs may be expanded or exceptions may be taken by following the Statewide Policy Exception Procedure.

4.1.1 Existing IT Products and Services

a. BU subject matter experts (SMEs) should inquire with the vendor and the state or agency procurement office to ascertain if the contract provides for additional products or services to attain compliance with PSPs prior to submitting a request for an exception in accordance with the Statewide Policy Exception Procedure.

4.1.2 IT Products and Services Procurement

a. Prior to selecting and procuring information technology products and services BU subject matter experts shall consider Statewide IT PSPs when specifying, scoping, and evaluating solutions to meet current and planned requirements.

5. ROLES AND RESPONSIBILITIES

5.1 State Chief Information Officer (CIO) shall:

a. Be ultimately responsible for the correct and thorough completion of IT PSPs throughout all state BUs.

5.2 State Chief Information Security Officer (CISO) shall:

a. Advise the State CIO on the completeness and adequacy of the BU activities and documentation provided to ensure compliance with Statewide Information Technology PSPs throughout all state BUs;

b. Review and approve BU security and privacy PSPs and requested exceptions from the statewide security and privacy PSPs; and

c. Identify and convey to the State CIO the risk to state information systems and data based on current implementation of security controls and mitigation options to improve security.

5.3 BU Director shall:

a. Be responsible for the correct and thorough completion of Statewide Information Technology PSPs within the BU;

b. Ensure BU compliance with Access Control Policy; and

c. Promote efforts within the BU to establish and maintain effective use of state information systems and assets.

5.4 BU Chief Information Officer (CIO) shall:

a. Work with the BU Director to ensure the correct and thorough completion of Statewide Information Technology PSPs within the BU; and

b. Ensure Access Controls Policy is periodically reviewed and updated to reflect changes in requirements.

5.5 BU ISO shall:

a. Advise the BU CIO on the completeness and adequacy of the BU activities and documentation provided to ensure compliance with BU Information Technology PSPs;

b. Ensure the development and implementation of adequate controls enforcing the Access Controls Policy for the BU; and

c. Ensure all personnel understand their responsibilities with respect to the correct use and management of logical access controls for the protection of state information systems and assets.

5.6 Supervisors of state employees and contractors shall:

a. Ensure users are appropriately trained and educated on Access Control PSPs; and

b. Monitor employee activities to ensure compliance.

5.7 System Users of state information systems shall:

a. Become familiar with this policy and related PSPs; and

b. Adhere to PSPs regarding correct use and management of logical access controls for the protection of state information systems and assets.

6. STATEWIDE POLICY

6.1 **Access Enforcement** - The BU shall ensure the state information system enforces approved authorizations for logical access to information and system resources in accordance with applicable control policies (e.g., identity-based policies, role-based policies). [NIST 800-53 AC-3] [HIPAA 164.308(a)(3)(ii)(A) - Addressable, 164.308 (a)(4)(ii)(B) & (C) - Addressable]

6.1.1 (P) **Assign Responsibility** - The BU shall assign to an individual or team the security management responsibility of monitoring and controlling all access to Confidential data. [PCI DSS 12.5.5]

6.2 (P) **Develop Access Control Operational Procedures** - The BU shall develop daily operational security procedures that are consistent with requirements in this specification. [PCI DSS 12.2]

6.3 (P) **Information Flow Enforcement** - The BU shall ensure the state information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on BU-defined information flow control policies, including Policy 8350, Systems and Communications Protections. These policies prohibit direct public access between the Internet and any system component in the Protected state information system. [NIST 800-53 AC-4] [IRS Pub 1075] [PCI DSS 1.3]

6.3.1 (P) **Perimeter Firewalls for Wireless Networks** - The BU shall install perimeter firewalls between any wireless network and the Protected state information system, and configures these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the Protected state information system. [PCI DSS 1.2.3]

6.3.2 (P) **Personal Firewalls** - The BU shall require personal firewall software on any mobile device and/or employee-owned computers with direct connectivity to the Internet which are used to access the BU's network. [PCI DSS 1.4]

6.4 (P) **Least Privilege** - The BU shall employ the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. [NIST 800-53 AC-6] [IRS Pub 1075] [PCI DSS 7.1]

6.4.1 (P) **Organizational Isolation** - The BU shall implement policies and procedures that protect Confidential information from unauthorized access by other (e.g., larger BU to which the BU is a part of) organizations. [HIPAA 164.308 (a)(4)(ii)(A)]

6.4.2 (P) **Privileged Accounts** - The BU shall restrict access rights to privileged user accounts to least privileges necessary to perform job responsibilities. [PCI 7.1.1]

6.4.3 (P) **Job Classification** - The BU shall restrict access rights based on individual personnel's job classification and function. [PCI DSS 7.1.2]

6.5 (P) **Authorize Access to Security Functions** - The BU shall explicitly authorize access to the following security functions and security-relevant information: [NIST 800-53 AC-6(1)] [IRS Pub 1075]

a. Establishing system accounts

b. Configuring access authorizations

c. Setting events to be audited

d. Setting intrusion detection parameters

e. Filtering rules for routers and firewalls

f. Cryptographic key management information

g. Configuration parameters for security services

6.6 (P) **Non-Privileged Access for Non-Security Functions** - The BU shall require that users of state information system accounts, or roles, with access to security functions (e.g., privileged users), use non-privileged accounts or roles, when accessing non-security functions. [NIST 800-53 AC-6(2)] [IRS Pub 1075]

6.7 (P) **Auditing of Privileged Functions** - The BU shall include execution of privileged functions in the events to be audited by the state information system. [NIST 800-53 AC-6(9)]

6.8 (P) **Prohibit Non-Privileged Users From Executing Privileged Functions** - The BU shall ensure the state information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures. [NIST 800-53 AC-6(10)] [IRS Pub 1075]

6.9 **Unsuccessful Logon Attempts** - The BU shall ensure the state information system enforces a BU specified limit of consecutive invalid logon attempts by a user; and automatically locks the account/node for a BU specified period of time or locks the account/node until released by an administrator when the maximum number of unsuccessful attempts is exceeded, consistent with the Access Control Standard 8320. [NIST 800-53 AC-7] [PCI DSS 8.5.13]

6.10 **System Use Notification** - The BU shall ensure the state information system: [NIST 800-53 AC-8]

6.10.1 Displays to users a BU-defined notification banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, state laws, Executive Orders, directives, policies, regulations, standards, and guidance and shall state the following:

a. Users are accessing a state information system owned by the State of Arizona;

b. State information system usage may be monitored, recorded, and subject to audit;

c. Unauthorized use of the state information system is prohibited and subject to criminal and civil penalties; and

d. Use of the state information system indicates consents to monitoring and recording.

e. Retains the notification banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the state information system; and

f. For publicly accessible systems; the state information system shall also:

g. Display to users the system use state information before granting further access;

h. Display to users references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and

i. Include in the notice given to public users of the state information system, a description of the authorized uses of the system.

6.11 (P) **Session Lock** - The BU shall ensure the state information system prevents further access to the system by initiating a BU specified limit of time inactivity or upon receiving a request from a user; and retains the session lock for a BU specified limit of time or until the user reestablishes access using established identification and authentication procedures. If the user does not reestablish access within a BU specified limit of time the session is dropped. [NIST 800-53 AC-11] [IRS Pub 1075] [HIPAA 164.312 (a)(2)(iii)] [PCI DSS 8.5.14, 8.5.15]

6.12 **Permitted Actions Without Identification or Authentication** - The BU shall identify user actions that can be performed on the state information system without identification or authentication consistent with BU missions; and documents and provides support rationale in the security plan for the state information system, user actions not requiring identification or authentication. [NIST 800-53 AC-14]

6.13 **Remote Access** - The BU shall establish usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and authorizes remote access to the state information system prior to allowing such connections. [NIST 800-53 AC-17]

6.13.1 (P) **Automated Monitoring / Control** - The BU shall ensure the state information system monitors and controls remote access methods (e.g., detection of cyber-attacks such as false logins and denial of service-attacks and compliance with remote access policies such as strength of encryption). [NIST 800-53 AC-17(1)] [IRS Pub 1075]

6.13.2 (P) **Security Using Encryption** - The BU shall ensure the state information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions, consistent with the System and Communication Protection Standard 8350. [NIST 800-53 AC-17(2)] [IRS Pub 1075] [PCI DSS 2.3, 4.1]

6.13.3 (P) **Managed Access Control Points** - The BU shall ensure the state information system routes all remote accesses through a limited number of managed network access control points. [NIST 800-53 AC-17(3)] [IRS Pub 1075]

6.13.4 (P) **Privileged Access Commands** - The BU shall authorize the execution of privileged commands and access to security-relevant information using

remote access only for BU-defined needs, and documents the rationale for such access in the security plan for the state information system. [NIST 800-53 AC-17(4)] [IRS Pub 1075]

6.14 Wireless Access - The BU shall establish usage restrictions, configuration/connection requirements, and implementation guidance for wireless access; and authorizes wireless access to the state information system prior to allowing such connections that are consistent with the System and Communication Protection Standard 8350. [NIST 800-53 AC-18]

6.14.1 (P) **Wireless Authentication and Encryption** - The BU shall ensure the state information system protects wireless access to the state information system using authentication of users and devices and encryption. [NIST 800-53 AC-18(1)] [IRS Pub 1075] [PCI DSS 4.1]

6.15 Access Control for Mobile Devices - The BU shall establish usage restrictions, configuration/connection requirements, and implementation guidance for BU controlled mobile devices; and authorizes connection of mobile devices to state information systems. [NIST 800-53 AC-19]

6.15.1 (P) **Full Device Encryption** - The BU shall employ full-device encryption to protect the confidentiality and integrity of information on mobile devices authorized to connect to state information systems or to create, transmit or process Confidential information. [NIST 800-53 AC-19(5)] [IRS Pub 1075] [HIPAA 164.308 (e)(2)(ii) - Addressable] [PCI DSS 4.1]

6.16 Use of External Information Systems - The BU shall establish terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to access the information system from external information systems; and process, store, or transmit BU controlled information using external information systems. [NIST 800-53 AC-20]

6.16.1 (P) **Limits on Authorized Use** - The BU shall permit authorized individuals to use an external information system to access the state information system to process, store, or transmit BU controlled information only when the BU: [NIST 800-53 AC-20(1)] [IRS Pub 1075]

a. Verifies the implementation of required security controls on the external system as specified in the BUs information security policies and security plan; or

b. Retains approved information system connection or processing agreements with the organizational entity hosting the external information system.

6.16.2 (P) **Portable Storage Devices** - The BU shall restrict or prohibit the use of BU controlled portable storage devices by authorized individuals on external information systems. [NIST 800-53 AC-20(2)] [IRS Pub 1075]

6.17 (P) **Information Sharing** - The BU shall facilitate information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for BU-defined circumstances; and shall employ mechanisms or processes to assist users in making information sharing/collaboration decisions. [NIST 800-53 AC-21] [IRS Pub 1075] [PCI DSS 12.8]

6.17.1 (P) **Maintain List of Service Providers** - The BU shall maintain a list of service providers that have access to Confidential data. [PCI DSS 12.8.1]

6.17.2 (P) **Written Agreements** - The BU shall maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of Confidential data the service providers possess. [PCI DSS 12.8.2]

6.17.3 (P) **Due Diligence** - The BU shall ensure there is an established process for engaging service providers including proper due diligence prior to engagement. [PCI DSS 12.8.3]

6.17.4 (P) **Service Provider Monitoring Program** - The BU shall maintain a program to monitor service provider's compliance with requirements for the protection of Confidential data. [PCI DSS 12.8.4]

6.18 Publicly Accessible Content - The BU shall: [NIST 800-53 AC-22]

a. Designate individuals authorized to post information onto a publicly accessible information system;

b. Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information;

c. Review the proposed content of information prior to posting onto the publicly accessible state information system to ensure that nonpublic information is not included; and

d. Review the content on the publicly accessible state information system for nonpublic information annually and removes such information, if discovered.

7. DEFINITIONS AND ABBREVIATIONS

7.1 Refer to the PSP Glossary of Terms located on the ADOA-ASET website.

8. REFERENCES

8.1 Statewide Policy Exception Procedure

8.2 STATEWIDE POLICY FRAMEWORK 8350, Systems and Communications Protections

8.3 Statewide Standard 8320, Access Control

8.4 Statewide Standard 8350, System Communication and Protection

8.5 NIST 800-53 Rev. 4, Recommended Security Controls for Federal Information Systems and Organizations, February 2013.

8.6 HIPAA Administrative Simplification Regulation, Security and Privacy, CFR 45 Part 164, February 2006

8.7 Payment Card Industry Data Security Standard (PCI DSS) v2.0, PCI Security Standards Council, October 2010.

8.8 IRS Publication 1075, Tax Information Security Guidelines for Federal, State, and Local Agencies: Safeguards for Protecting Federal Tax Returns and Return Information, 2010.

9. ATTACHMENTS

None.

10. REVISION HISTORY

Date	Change	Revision	Signature
5/1/14	Initial Release	DRAFT	Aaron Sandeen, State CIO and Deputy Director